

## USAREUR COMPUTER-USER AGREEMENT

This appendix is a reference copy of the USAREUR Computer-User Agreement on the Regional Computer Emergency Response Team, Europe (RCERT-E) webpage at <http://www.rcerte.5sigcmd.army.mil>. Your systems administrator or information systems security officer will ask you to sign a copy of this agreement before issuing you a password.

\*\*\*\*\*

As a user of a USAREUR automated information system, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any Government-owned software or install hardware on any Government computer (GC) (for example, client-workstation, server) without first getting written approval from my commander, SA, or IASO.
3. I will not load any software onto my GC, Government information technology (IT) system, or network without the approval of my commander, SA or IASO.
4. I will not try to access data or use operating systems or programs, except as specifically authorized.
5. I know I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them-
  - a. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report to my SA for a new one.
  - b. If I have a classified account, I will ensure that my password is changed at least once every 90 days or if compromised, whichever is sooner.
  - c. If I have an unclassified account, I will ensure that my password is changed at least once every 150 days or if compromised, whichever is sooner.
  - d. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.
  - e. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.

- f. I understand that if my password does not meet current Army in Europe standards, I am to inform my SA.
  - g. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or magnetic or electronic media.
  - h. I will not tamper with my GC to avoid adhering to Army in Europe password policy.
  - i. I will never leave my classified GC unattended while I am logged on unless the GC is protected by a "password protected" screensaver.
- 6. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.
- 7. I know that if connected to the LandWarNet (Class), my system operates at least in the U.S. Secret, "system-high" mode.
  - a. Any magnetic media used on the system must be marked and protected immediately according to AR 380-5. In other words, any disk going into a Secret system is now Secret and must be handled accordingly.
  - b. Magnetic disks or compact disks will not be removed from the computer area without the approval of the local commander or head of the organization.
  - c. I must protect all material printed out from the LandWarNet (Class) at the Secret level until the information is downgraded or declassified.
  - d. I will not enter information into a system if the information has a higher classification than that for which the system is accredited.
  - e. If connected to the LandWarNet (Class), only U.S. personnel with a security clearance are allowed unescorted access to the system.
  - f. Foreign military representatives will not have access to a LandWarNet (Class) terminal.
  - g. NATO material stored, processed, or transmitted on a LandWarNet (Class) terminal must be protected according to AR 380-15
- 8. My local IASO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the SA or IASO.

9. I will scan all magnetic media (for example, disks, CDs, tapes, universal serial bus (USB) memory sticks) for malicious software (for example; viruses, worms) before using it on a GC, IT system, or network in the Army in Europe.
10. I will use only approved methods to “air gap” information from the LandWarNet (Class) or LandWarNet (Class).
11. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO and delete the message.
12. I will not run “sniffer” or any hacker-related software on my GC, Government IT system, or network.
13. I will not download file-sharing software (including MP3 music and video files) or games onto my GC, Government IT system, or network.
14. I will not connect any personal IT equipment (for example, PEDs and PDAs (such as Palm Pilots), personal computers, digitally enabled devices) to my GC or to any Government network without the written approval of my commander, SA, or IASO and IMO.
15. I will ensure that my anti-virus software on my GC is updated at least weekly.
16. I will not use Internet “chat” services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my AKO account.
17. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.
18. I will comply with security guidance issued by my SA and IASO.
19. If I have a public key infrastructure (PKI) certificate installed on my computer (for example, software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.
20. I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.
21. I know I am subject to disciplinary action if I violate Army in Europe computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice

(UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations, or host-nation laws.

PLEASE READ THE BELOW PARAGRAPHS: WHEN YOU SIGN THIS AGREEMENT YOU ARE IN FACT STATING THAT YOU FULLY UNDERSTAND THE OPSEC MESSAGE WHICH IS INSERTED.

Subj: (U) CHIEF OF STAFF OF THE ARMY OPSEC GUIDANCE (U//FOUO)  
(U//FOUO) THE ENEMY IS ACTIVELY SEARCHING THE UNCLASSIFIED NETWORKS FOR INFORMATION, ESPECIALLY SENSITIVE PHOTOS, IN ORDER TO OBTAIN TARGETING DATA, WEAPONS SYSTEM VULNERABILITIES, AND TTPs FOR USE AGAINST THE COALITION. A MORE AGGRESSIVE ATTITUDE TOWARD PROTECTING FRIENDLY INFORMATION IS VITAL TO MISSION SUCCESS. THE ENEMY IS A PRO AT EXPLOITING OUR OPSEC VULNERABILITIES.

2. (U//FOUO) IT IS CRITICAL TO REMIND OUR PEOPLE THAT THE NEGLIGENT OR UNAUTHORIZED RELEASE OF SENSITIVE PHOTOS IS A SERIOUS THREAT TO OUR FORCES. LEADERS ARE ENCOURAGED TO:

2.A. (U//FOUO) REMIND ALL PERSONNEL THAT THE ENEMY WILL EXPLOIT SENSITIVE PHOTOS SHOWING THE RESULTS OF IED STRIKES, BATTLE SCENES, CASUALTIES, DESTROYED OR DAMAGED EQUIPMENT, AND ENEMY KIAs AS PROPAGANDA AND TERRORIST TRAINING TOOLS. FOR EXAMPLE, ANNOTATED PHOTOS OF AN ABRAMS TANK PENETRATED BY AN RPG ARE EASILY FOUND ON THE INTERNET. CAPTURED INSURGENT PAMPHLETS CONTAIN HAND DRAWINGS AND INSTRUCTIONS ON WHAT INSURGENTS BELIEVE ARE VULNERABLE PENETRATION POINTS ON TANKS, HMMWVS, BRADLEY FIGHTING VEHICLES, AND HELICOPTERS. RELEASING PHOTOS OUTSIDE OFFICIAL, PROTECTED CHANNELS MAY ALLOW THE ENEMY MATERIAL FOR HIS INFORMATION OPERATIONS AND TARGETING TTP AGAINST FRIENDLY FORCES. INSURGENTS ALSO USE WEBSITES TO COMMUNICATE, TRAIN, AND RECRUIT FOLLOWERS, OFTEN USING PHOTOS/VIDEO OF THEIR BATTLEFIELD SUCCESSES. WE CANNOT AFFORD TO HAVE OUR PHOTOS BECOME TRAINING AND RECRUITMENT TOOLS FOR THE ENEMY.

2.B. (U//FOUO) INFORM YOUR PERSONNEL THAT WE COULD UNWITTINGLY MAGNIFY ENEMY CAPABILITIES SIMPLY BY EXCHANGING PHOTOS WITH FRIENDS, RELATIVES, OR BY PUBLISHING THEM ON THE INTERNET OR OTHER MEDIA. WE ARE NOT LIMITING AUTHORIZED COMMUNICATION (TO INCLUDE THE APPROPRIATE USE OF PHOTOS) UNDER EXISTING PUBLIC AFFAIRS GUIDANCE, BUT WE MUST PROTECT PHOTOS THAT REVEAL TO THE ENEMY OUR BATTLE LOSSES, ONGOING FRIENDLY OPERATIONS, TTP, EQUIPMENT VULNERABILITIES, OR DISCLOSE INTELLIGENCE COLLECTION EFFORTS AND METHODS. MOREOVER, WE MUST PROTECT INFORMATION THAT MAY HAVE A NEGATIVE IMPACT ON FOREIGN RELATIONS WITH COALITION ALLIES OR WORLD OPINION.

3. (U//FOUO) OUR MISSION SUCCESS AND SOLDIERS LIVES DEPEND ON AGGRESSIVELY DENYING THE ENEMY ANY ADVANTAGE. I NEED YOUR FOCUS ON THIS CRITICAL ISSUE.

COMPUTER: \_\_\_\_\_  
USER NAME \_\_\_\_\_

SECURITY \_\_\_\_\_  
OFFICER NAME \_\_\_\_\_

DATE \_\_\_\_\_

DATE \_\_\_\_\_